Health IT Standards Committee

A Public Advisory Body on Health Information Technology to the National Coordinator for Health IT

April 12, 2011

Farzad Mostashari, MD
National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Dr. Mostashari:

The HIT Standards Committee (Committee) gave the following broad charge to the Privacy & Security Standards Workgroup (Workgroup):

Broad Charge for the Privacy & Security Standards Workgroup:

- The Privacy & Security Standards Workgroup is charged with making recommendations to the HIT Standards Committee on privacy and security requirements that should be included in standards, certification criteria, and implementation specifications.

Since January 2011, the Workgroup conducted a number of public meetings and presentations from users (i.e., VA Health System, ONC Direct Project, Nw-HIN) regarding digital certificates. On March 29, 2011, the Workgroup reported and discussed its findings with the Committee, which were subsequently approved.

This letter provides recommendations to the Department of Health and Human Services (HHS) on the issue of digital certificates.

Background and Discussion

An important strategic goal of the Office of the National Coordinator (ONC) is to build public trust and participation in health information technology (IT) and electronic health information exchange by incorporating effective privacy and security into every phase of health IT development, adoption, and use. The Workgroup was tasked to recommend requirements and evaluation criteria for standards for digital certificates, which are used to create high-level assurance that an organization exchanging health information is the entity it claims to be (authentication). Digital certificates are used by both Nw-HIN and ONC Direct exchanges to authenticate entities involved in health data exchanges.

RECOMMENDATIONS ON DIGITAL CERTIFICATES

The following recommendations apply to digital certificates:

1. Recommendations on the requirements and evaluation criteria for digital certificates.

- (1a) Recommended Requirements:
  - Digital certificates must conform to the X.509 V3 certificate profile defined in RFC 5280 (May 2008)
  - Digital certificates to support Direct exchanges:
  - MUST include the set of Basic Certificate Fields defined in Section 4.1 of RFC 5280
  - MUST include Standard Extensions required to support the simple mail transfer protocol (SMTP) with Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - MAY include additional Standard Extensions as defined in Section 4.2 of RFC 5280
  - Digital certificates to support NW-HIN exchanges:
  - MUST include the set of Basic Certificate Fields defined in Section 4.1 of RFC 5280
  - MUST include Standard Extensions required to support mutually authenticated transport layer security (TLS) connections
  - MAY include additional Standard Extensions as defined in Section 4.2 of RFC 5280
  - Certificate revocation lists (CRLs) MUST conform to the X.509 V2 CRL profile defined in Section 5 of RFC 5280 (which supports both Online Certificate Status Protocol (OCSP) and full CRL retrieval)

- (1b) Recommended Evaluation Criteria
  - Does the standard conform to the X.509 V3 profile defined in RFC 5280?
  - Does the standard specify the Basic Certificate Fields and Extensions as REQUIRED for Direct exchanges?
  - Does the standard specify the Basic Certificate Fields and Extensions as REQUIRED for NW-HIN exchanges?
  - If the standard includes one or more additional Extensions, are these as specified in the Standard Certificate Extensions defined in RFC 5280?
  - If the standard includes Extensions applicable only to Direct or NW-HIN exchanges, are the intended usage of these Extensions clear and unambiguous?
  - Does the standard include X.509 V2 certificate revocation lists (CRLs) as defined in RFC 5280?
  - Is the standard specified clearly and completely enough for a developer to implement?

2. Recommendation to ONC: To enable Direct users to exchange health information with federal health agencies, the HIT Standards Committee recommends that the ONC investigate architectural and operational alternatives for cross-certifying Health ISPs (HISPs) with the Federal Bridge Certificate Authority (CA), including an examination of potential benefits and implications on cost, market dynamics, and complexity.

  - *There is a need for investigation of alternatives for cross-certifying digital certificate issuers with the Federal Bridge, which is important for interoperability between non-Federal and Federal organizations.*

3.Recommendation to the HIT Policy Committee: In the attached document, we set forth the implications and concerns that arise from the current lack of policy and governance around establishing the trustworthiness of CAs that issue digital certificates to entities involved in Direct exchanges. We assert that:

- Policy and governance are needed around Certificate Authorities (CAs) who issue certificates for use in health exchanges, such as Direct.
- Such policy should define a mechanism for establishing the legitimacy and trustworthiness of a CA.
- Such policy should define a minimum level of trustworthiness for CAs issuing certificates for Direct exchanges; for example:
    - Is certification by WebTrust or European Telecommunications Standards Institute (ETSI) sufficient for health information exchange?
    - Does the CA need to meet the minimum standard defined for a trusted relationship with the Federal Bridge CA?

We appreciate the opportunity to provide these recommendations on digital certificates, and look forward to discussing next steps.

Sincerely yours,

/s/
Jonathan Perlin
Chair, HIT Standards Committee

/s/
John Halamka
Vice Chair, HIT Standards Committee

Attachment: Recommendation 3

HIT Standards Committee:
Digital Certificate Trust –
Policy Question for HIT Policy Committee

March 29, 2011

INTRODUCTION TO DIGITAL CERTIFICATES AND CERTIFICATE TRUST

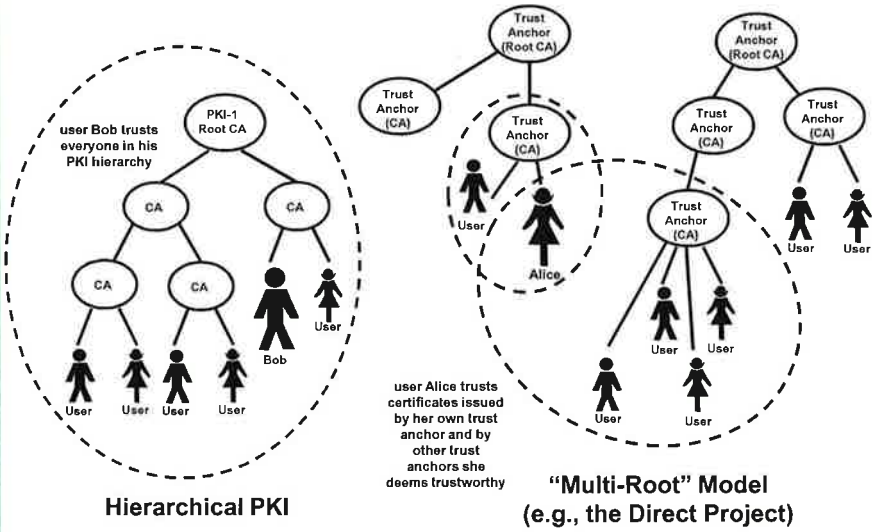
Digital Certificate Basics

- A "digital certificate" is an electronic document that certifies that the subject (person or entity) has been issued a pair of encryption keys that are related in such a way that if one key is used to encrypt something (e.g., file, message, data stream), it can be decrypted only by someone holding the other key
  - One key is published for anyone to see ("public key")
  - The other key is kept secret by the entity/person to whom the digital certificate has been issued ("private key")
  - Digital certificates are issued by a "certificate authority" (CA) – and digitally signed by the issuing CA
    - CA certificates may be self-issued and self-signed certificates
- CAs periodically publish a "certificate revocation list (CRL)" that identifies those certificates that no longer are valid and that have not expired

Digital Certificate Basics

- Digital certificates are used for a number of purposes, including:
  - To authenticate the identity of an entity or person using a challenge-response mechanism
  - To digitally sign a message or other transmitted content ("digital signature")
  - To share a secret key to be used to exchange private or sensitive information
- The trustworthiness of a digital certificate is dependent upon how much the user trusts the issuer of the certificate – which may be the top CA in a hierarchical public key infrastructure (PKI), the CA that issued the user's own certificate, or any other trusted CA
  - The practices used by a CA in issuing and managing certificates are described in its Certification Practice Statement (CPS)
  - CPSs may be certified by organizations such as the European Telecommunications Standards Institute (ETSI) and WebTrust, or as meeting minimal standards established by specific communities, such as SAFE Bio-Pharma and Federal Bridge

Digital Certificate Trust Models



Digital Certificate Content

Signature of CA that issued certificate
Algorithm used by the CA to sign the certificate
Version
Serial number
Name of the CA that issued certificate
Period of time for which the certificate is valid
Name of the subject to whom the certificate is issued
The subject's public key
Optional extensions – such as the purposes for which the certificate may be used

Certificate Trust Issue

- A digital certificate can be trusted only to the extent to which the user trusts the CA who issued the certificate
- Anyone can set themselves up as a CA and issue certificates
- Certificates used by Direct Project entities may be issued by any CA – and the decision of whether to trust the certificate is left up to the communicating entity's trust relationship with the issuing CA (i.e., whether the CA is recognized as a "trust anchor")
- To exchange information with federal entities (e.g., VA, CMS), the user will need to hold a certificate that was issued by a CA that is trusted by the Federal Bridge CA

POLICY QUESTION FOR HIT POLICY COMMITTEE

Policy Question for HITPC

- Policy and governance are needed around CAs who issue certificates for use in health exchanges, such as Direct
  - Defining a mechanism for establishing the legitimacy and trustworthiness of a certificate authority
  - Defining a minimum level of trustworthiness for CAs issuing certificates for Direct exchanges; for example:
    - Is certification by WebTrust or ETSI sufficient for health information exchange?
    - Does the CA need to meet the minimum standard defined for a trusted relationship with the Federal Bridge CA?